UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,004	08/17/2001	Nang Kon Kwan	06502.0336	2756

22852 7590 08/04/2005

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
CHAI, LONGBIT	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 08/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/931,004	KWAN, NANG KON	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 June 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10,12-21,25-28 and 30-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10,12-21,25-28 and 30-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1 – 33 have been presented for examination. Claims 11, 22 – 24 and 29 have been canceled; claims 1 – 8, 10, 12, 14 – 17, 19, 21, 26, 28, 30 and 33 have been amended in an amendment filed 6/17/2005. Therefore, presently pending claims are 1 – 10, 12 – 21, 25 – 28 and 30 – 33.

Response to Arguments

1. Applicant's arguments filed on 06/17/2005 with respect to the subject matter of the instant claims have been fully considered but are not persuasive. See the same reasons as the response set forth in the following Office action.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1 – 10, 12 – 21, 25 – 28 and 30 – 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bisbee (Patent Number: 6367013), in view of CFSB ("How Key Escrow Might Work", by Computer Fraud & Security Bulletin, July 1, 1996).

As per claim 1, 15 and 33, Bisbee teaches method in a data processing system for requesting a digital certificate from a certificate authority and archiving an encryption key outside of the certificate authority, comprising:

receiving a request from a user for a digital certificate, the request including an encryption key associated with the user (Bisbee: Column 12 Line 27 – 28 and Column 11 Line 52 – 66: the public key is used as the basis for a certificate request, where the basis is uniquely associated with a key-pair assigned to a user).

Bisbee does not teach providing an indication of proof of storing the encrypted user's encryption key, wherein the indication of proof is signed with a second archival key.

CFSB teaches providing an indication of proof of storing the encrypted user's encryption key, wherein the indication of proof is signed with a second archival key (CSFB: 1st Para Line 5 – 7 and 4th Para Line 1 – 2: the key escrow certificate is served as the indication of proof that the key has been escrowed when provided to CA as taught by CFSB);

encrypting the user's encryption key with a first archival key (CFSB: 10th Para Line 1 – 2 and 7th Para Line 1 – 2);

storing the encrypted user's encryption key in a database under the control of a first entity separate from the certificate authority (CSFB: 1st Para Line 5 – 7, 4th Para Line 1 – 2 and 10th Para Line 1 – 2: CSFB teaches the key escrow agent could be different from the CA);

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of CFSB within the system of Bisbee because (a) Bisbee teaches digital certificate management mechanisms through a registration manager (RM) (Bisbee: Column 11 Line 20 – Column 12 Line 29 and Figure 2) and (b) CFSB teaches a more flexible and security enhanced method to manage the digital certificate in the sense that users could choose a secure independent 3rd party as an key escrow agent (different from the CA) that is certified as meeting the standard to provide a high level of assurance that keys are not compromised or misused (CFSB: see for example, 1st Para Line 5, 4th Para Line 1 – 2 and 6th Para Line 1 – 2).

Accordingly, Bisbee in view of CFSB teaches:

verifying the signed indication of proof based on the first archival key (Bisbee: Column 12 Line 27 & CSFB: 1st Para Line 5 – 7: (a) Registration Manager (RM) is the requesting entity (Bisbee: Column 12 Line 27 – 28) and thereby the digitally signed indication of proof (CFSB: Column 12 Line 27 – 28) must be first responded back to the requester so that the sender (RM) can verify the indication of proof is indeed performed and sent by the authorized key escrow agent certified as meeting the standards (CFSB: 4th Para Line 1 – 2), (b) the key escrow certificate is served as the indication of proof which is digitally signed by the key escrow agent as taught by CFSB); and

providing the request to the certificate authority based on the verification of the signed indication of proof (Bisbee: Column 12 Line 27 & CSFB: 1st Para Line 5 – 7).

As per claim 2 and 20, Bisbee as modified teaches sending a digital certificate from the certificate authority to the user in response to the certificate authority receiving request (CFSB: see for example, 1st Paragraph).

As per claim 3, Bisbee as modified teaches encrypting the user's encryption key with a first archival key is performed by the first entity (CFSB: 10th Para Line 1 – 2 and 7th Para Line 1 – 2).

As per claim 4, 5 and 21, Bisbee as modified teaches encrypting the request with a transport key; and sending the transport encrypted request to the first entity (CFSB: 7th Para Line 4: CFSB teaches using the recipient's public key to encrypt the transmitted message).

As per claim 6, Bisbee as modified teaches the first entity is a data recovery manager (CFSB: 7th Para Line 1 – 4: key holder (or key escrow agent) is indeed the "data recovery manager") that receives and manages archiving of the encryption key, and wherein the transport key is the data recovery manager's public transport key (CFSB: 7th Para Line 1).

As per claim 7, 13, 25 and 31, Bisbee as modified teaches the second archival key is a data recovery manager private key (CSFB: 1st Para Line 6 – 7: the indication of

proof is digitally signed by the key holder (or key escrow agent), where the private key must be used for digital signature).

As per claim 8 and 26, the claim limitations are met as the same reasons set forth in the paragraph above regarding to claim 1 with the exception of the feature wherein verifying the signed indication of proof is performed by a second entity separate from the first entity and the certificate authority (Bisbee: Column 12 Line 27 & CSFB: 1st Para Line 5 – 7: (a) Registration Manager (RM) is the requesting entity (Bisbee: Column 12 Line 27 – 28) and thereby the digitally signed indication of proof (as taught by CFSB – see above) must be first responded back to the requester so that the sender (RM) can verify the indication of proof is indeed performed and sent by the authorized key escrow agent certified as meeting the standards (CFSB: 4th Para Line 1 – 2), (b) the key escrow certificate is served as the indication of proof which is digitally signed by the key escrow agent as taught by CFSB (c) CFSB teaches users could choose a secure 3rd party as an key escrow agent (different from the CA) to archive the keys that is certified as meeting the standard to provide a high level of assurance that keys are not compromised or misused (CFSB: see for example, 1st Para Line 5, 4th Para Line 1 – 2 and 6th Para Line 1 – 2)).

As per claim 9, 14, 27 and 32, Bisbee as modified teaches the user's encryption key is archived under control of the user (CFSB: 4th Para Line 1 – 2)

As per claim 10, 12, 16, 17, 18, 28 and 30, the claim limitations are met as the same reasons set forth in claim 1.

As per claim 19, the claim limitations are met as the same reasons set forth in claim 1, 4 and 6.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LBC

Longbit Chai
Examiner
Art Unit 2131

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100